The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

Paper No. 23

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Ex parte LUCIANO CHAVEZ

Appeal No. 2004-1678
Application 09/292,190[1]

ON BRIEF

Before BARRETT, RUGGIERO, and BLANKENSHIP, Administrative Patent Judges.

BARRETT, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134(a) from the final rejection of claims 1-7, 12-17, 21, and 22. Claims 8-11 and 18-20 have been allowed (Paper No. 14).

We reverse.

[1] Application for patent filed April 15, 1999, entitled "Method and System for Enabling a Network Function in a Context of One or All Server Names in a Multiple Server Name Environment."

BACKGROUND

The invention relates to a method of executing a function on a server in a distributed data processing system. The server responds to requests directed to a set of server names. A function request has an input that specifies a server name in the set of server names. The server name context on the server has a set of resources associated with the server name. A server name mask is generated based on the server name specified in the function request and the function is executed in a server name context on a server based on the generated server name mask.

Claim 1 is reproduced below.

> 1. A method for executing a function on a server in a distributed data processing system, the method comprising the computer-implemented steps of:
>
> receiving a request for a function, wherein the request comprises an input specifying a server name, wherein the server responds to requests directed to a set of server names;
>
> generating a server name mask based on the server name; and
>
> executing the function in a server name context on the server, as directed by the input specifying the server name, based on the generated server name mask.

THE REFERENCES

The examiner relies on the following references:

Nishimoto et al. (Nishimoto)	6,199,164	March 6, 2001 (filed January 9, 1998)
French et al. (French)	6,442,685	August 27, 2002 (March 31, 1999)

THE REJECTION

Claims 1-7, 12-17, 21, and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over French and Nishimoto.

We refer to the final rejection (Paper No. 14) (pages referred to as "FR__") and the examiner's answer (Paper No. 19) (pages referred to as "EA__") for a statement of the examiner's rejection, and to the appeal brief (Paper No. 18) (pages referred to as "Br__") and reply brief (Paper No. 20) (pages referred to as "RBr__") for a statement of appellant's arguments thereagainst.

OPINION

The rejection and arguments

The examiner finds (FR1; EA3) that French discloses the limitation of "receiving a request for a function, wherein the request comprises an input specifying a server name, wherein the server responds to requests directed to a set of server names." This finding is not in dispute. The examiner finds that French does not disclose "generating a server name mask based on the server name; and executing the function in a server name context on the server, as directed by the input specifying the server name, based on the generated server name mask," but that these limitations are disclosed by Nishimoto, "i.e., [a] masking process based [on] the retrieval acceptance from the host server name 218, see figs. 7, 20A and 20B, abstract, col. 12 line 20 to

col. 13 line 60 and col. 23 line 1 to col. 24 line 60" (FR1; EA4). The examiner concludes that it would have been obvious "to implement Nishimoto's teachings into the computer system of French to control the transmission data because it would have provided a masking process to the personal access information and provided a more secure network environment" (FR1-2; EA4). The examiner further states that "Nishimoto discloses masking process based the retrieval acceptance from the host server name and generating a permission IP server host name and a refusal IP server host name" (italics omitted) (EA6).

Appellant argues that Nishimoto does not teach "generating a server name mask based on the server name; and executing the function in a server name context on the server, as directed by the input specifying the server name, based on the generated server name mask" as recited in claims 1, 12, and 21. Appellant addresses in detail, both in the brief and reply brief, the portions of Nishimoto relied upon by the examiner to show masking. In regard to the examiner's statement about "generating a permission IP server host name and a refusal IP server host name" (EA6), appellant argues that it is not clear what element in Nishimoto the examiner believes is the same as the server name mask, but appellant again argues the teachings of Nishimoto (RBr2-5). It is further argued that there is no suggestion to combine French and Nishimoto to arrive at the claimed invention.

Although appellant also addresses the separate patentability of the group consisting of claims 5 and 16 and the group consisting of claims 6 and 17, it is unnecessary to reach these arguments.

The "mask" teachings of Nishimoto

Nishimoto discloses a connection server 12 for controlling the connection between a peer client 10 of a user and an IP server 14 on an open network. The connection server receives access permission information at the start of the connection of a peer client, registers the access permission information into a database, and responds with the relevant access permission information for a retrieval request from an IP server (abstract). The peer client has three reception channels: an emergency channel 86, a regular confirmation channel 68, and a preservation channel 70 for displaying received information from the IP server onto display 26 (Fig. 2A; col. 10, lines 13-39). The connection server 12 stores connection information 94 having an ID, an IP address, and passwords for each of the three channels (Fig. 4; col. 11, lines 11-23). The opening and non-opening of the channels are controlled in accordance with the designation of connection permission information (col. 11, lines 24-28), which uses the masking process. The connection server 12 also stores connection permission information 96, where permission IP server host names and a refusal IP server host names can be registered

into each of the connection permission information of the three channels (Fig. 5; col. 11, lines 29-49).

The masking process is illustrated by example. The connection permission information 96 may start out as shown in Fig. 17C with allowing communication to "NONE" of the IP servers on the emergency channel and allowing communication to "ALL" IP servers on the regular confirmation channel. The connection information 94-1 with passwords to each of the three channels is shown in Fig. 17D. When the connection server 12 receives a request from an IP server 14 for connection information to connect to a peer client 10 having a certain ID, the connection server masks the connection information 94-1 (Fig. 17D) using the connection permission information 96 (Fig. 17C) to form the transmitted connection information 94-2 (Fig. 17E; Fig. 16A, S108). In this case, the masking process masks the password 130 of the emergency channel and password 132 of the regular confirmation channel are masked by masks 212 and 214, respectively because the connection permission information 96 (Fig. 17C) is "NONE" for these channels, and the password 134 of the reservation channel is not masked because the connection permission information 96 is set to "ALL" (col. 20, lines 38-56; passwords misnumbered). The IP server would transmit to the peer client on the preservation channel (Fig. 16A, S206).

As a second example, the client may edit the permission information to permit real estate companies to use the emergency channel (Fig. 18A, S1; Fig. 19A). When the IP server requests connection information from the connection server (Fig. 18A, S202), the connection server refers to the connection permission information (Fig. 18B, S104), masks the connection information 94-1 (Fig. 19C) to form the transmitted connection information 94-2 (Fig. 19D). In this case, the password 130 of the emergency channel, which was masked (Fig. 17C), is released or unmasked (col. 22, lines 8-28).

As a third example, the client edits the permission information to permit I company to use the emergency channel, and to refuse J company to use the regular confirmation channel and the preservation channel (Fig. 20A, S4; col. 23, lines 14-19). The connection permission information file 96 in the connection server 12 is shown in Fig. 22B. In response to a request to retrieve connection information by the IP server (Fig. 21, S203), the connection server refers to the connection permission information 96, performs a masking process to mask channels, and returns the connection information to the IP server (Fig. 21, S103). Thus, in response to a request by the I company server, the connection server would send the connection information file 94-1 in Fig. 22B wherein none of the channels are masked (col. 24, lines 1-8), and in response to a request by the

J company server, the connection server would send the connection information file 94-2 in Fig. 2B wherein all of the channels are masked indicating that the user is not on the network (col. 24, lines 16-26).

Analysis

The examiner states in the response to argument section of the answer that "Nishimoto discloses masking process based the retrieval acceptance from the host server name and generating a permission IP server host name and a refusal IP server host name (see figs. 7, 20A and 20B, abstract, col. 12 line 20 to col. 13 line 60 and col. 23 line 1 to col. 24 line 60)" (italics omitted) (EA6). This does not explain how Nishimoto discloses the limitations of "generating a server name mask based on the server name; and executing the function in a server name context on the server, as directed by the input specifying the server name, based on the generated server name mask," which limitations appear in the independent claims. The permission IP server host name and refusal IP server host name are names of IP servers that are granted permission to connect to the peer client over a certain channel or that are refused permission to connect to the peer client over a certain channel, e.g., Fig. 22 shows a connection permission file 96 where I company is granted permission to connect on the emergency channel, all other IP servers are denied permission to connect on the emergency

channel, J company is denied permission to connect on the regular confirmation channel and the preservation channel, and all other IP servers are granted permission to connect on the regular confirmation channel and the reservation channel. No mask is disclosed with respect to specifying the IP servers. Figure 7, referred to by the examiner, shows registration of a plurality of IP server host names but says nothing about a mask or a server name mask. Figure 20A shows editing of connection permission information at step S4, and we know that the IP names will be used to create a password mask, but the examiner does not explain the relevance of Figs. 20A and 20B. The abstract says nothing about masking. Columns 12 to 13 discuss registering permission and refusal IP server host names, however the examiner does not explain how these two columns have anything to do with masking.

The only mask disclosed is masking the passwords for the three channels of the connection information file 94-1 using the permission IP server host name and the refusal IP server host name in the connection permission information file 96 when transmitting the connection information 94-2; see discussion of Figs. 17C to 17E, supra. As shown in Fig. 17E, the passwords of the emergency channel and the regular channel are masked. Masking is discussed at columns 23 to 24. This channel password mask is not a "server name mask" as claimed. Nor does the masking process disclose or suggest the step of "executing the

function in a server name context on the server, as directed by the input specifying the server name, based on the generated server name mask." Therefore, even if French and Nishimoto were combined, the combination would not teach all of the limitations of the independent claims. Furthermore, since Nishimoto does not teach what the examiner says it does, we cannot find motivation for the combination. Therefore, we conclude that the examiner has failed to establish a prima facie case of obviousness. The rejection of claims 1-7, 12-17, 21, and 22 is reversed.

REVERSED

LEE E. BARRETT
Administrative Patent Judge)

JOSEPH F. RUGGIERO
Administrative Patent Judge)

HOWARD B. BLANKENSHIP
Administrative Patent Judge)

BOARD OF PATENT APPEALS AND INTERFERENCES

IBM CORP (YA)
C/O YEE & ASSOCIATES PC
P.O. BOX 802333
DALLAS, TX 75380